ABELIAN GROUPS FORMED BY RESIDUES WITH RESPECT TO A DOUBLE MODULUS

BY

EDWARD AUGUST THEODORE KIRCHER
A. B. University of Illinois, 1911

THESIS

Submitted in Partial Fulfillment of the Requirements for the

Degree of

MASTER OF ARTS

IN MATHEMATICS

IN

THE GRADUATE SCHOOL

OF THE

UNIVERSITY OF ILLINOIS

1912

UNIVERSITY OF ILLINOIS

THE GRADUATE SCHOOL

May 29 1912

I HEREBY RECOMMEND THAT THE THESIS PREPARED UNDER MY SUPERVISION BY

Edward A. T. Kircher

ENTITLED Abelian groups formed by residues with respect to a double modulus

BE ACCEPTED AS FULFILLING THIS PART OF THE REQUIREMENTS FOR THE

DEGREE OF A. M.

G. A. Miller
In Charge of Major Work

E. J. Townsend
Head of Department

Recommendation concurred in:

Committee on Final Examination

INTRODUCTION.

It is the object of this paper to show the relation between abelian groups and the residue systems of a double modulus. Before proceeding it may be well to give a short outline of the developement of these two fundamental concepts. In 1770-1771 Lagrange wrote the wellknown "Réflexions sur la Résolution Algébraique des Equations"[1]) in which he summarized all that had been done until then toward finding general methods of solving algebraic equations. The first and second parts of the article are devoted to cubics and biquadratics, with general methods for the solution of both. In the case of equations of degree higher than the fourth he finds that nothing had been accomplished in reaching a solution by methods similar to those used for the third and fourth degrees. The only theories advanced that he regarded as being of any value are those of Tschiernaus and Euler, both of which require too much calculation to be of any practical use. Among those who tried to extend the results thus summarised by Lagrange was Paolo Ruffini who published several treatises and articles, chief among them being his "Teoria delle Equazioni", published at Bologna in 1799, in which he tries to approach the subject by a study of the number of values assumed by a rational integral function of several unknowns for all possible permutations of these unknowns, and by studying the totality of these permutations that leave the value of the function unchanged. In this way he developed a great deal of the theory of substitution groups and worked out five different proofs to show that equations of a degree higher than the fourth cannot be be solved by a general method.[2]) None of these proofs however is rigorous, and consequently although Ruffini was the first to develope the group principle and to have a perception of its value in solving the question under discussion, the distinction of having prooved it is awarded to Abel who in 1824 published a short outline of his proof in Christiania, and in 1826 the

[1]) Nouveaux Memoirs de l'Academie royale des Sciences et Belles-Lettres de Berlin, années 1770 et 1771.

[2]) See H. Burkhardt, Die Anfaenge der Gruppentheorie in Paolo Ruffini, Abh. zur Geschichte der Mathematik, Leipzig, 1892.

full proof.[3] Cauchy [4] was the first one to organize and clear up the results obtained by Ruffini, besides extending this new theory in several ways. The first one, however, to fully understand the fundamental laws underlying the results until then obtained was Galois [5], who helped to establish the study of finite groups in the modern manner. His work is "the starting point of a general group theory where only the laws of composition of the symbols constituting the group are placed in evidence. These symbols can be of any nature whatsoever, and represent numbers or number systems, or the systems of substitution already mentioned or even operations that are drawn from algebra, geometry, or mechanics"[6].

These general group laws may be stated in several ways, but the ones we shall make use of are the following: A number of elements forming a set following a certain law of combination shall be said to form a group when

1) Combining any two elements of the set gives another element of the set.
2) Combining any one element of the set with all the elements of the set gives back all the elements of the set.
3) The associative law of combination must hold, i.e. $a\circ(b\circ c)=(a\circ b)\circ c$.

For abelian groups we must also have that

4) The commutative law of combination must hold, i.e. $a\circ b=b\circ a$.

Whenever a certain number of the elements of a group form a group among themselves we have a subgroup of the general group. Whenever a one to one correspondence exists between the elements of two groups the groups are simply isomorphic. The order of any element is the number of times it must combine with itself before it repeats itself. The order of a group is equal to the number of elements contained in it. In the case of abelian groups, which is the only kind we shall consider, it is possible to find a set of elements

[3] Crelle's Journal, vol. I, 1826, p. 73. Works, Christiania 1881, p. 75.

[4] Mémoire sur le Nombre des Valeurs qu'une Fonction peut acquérir lorsqu'on y permute des toutes les manières possibles les quantités qu'elle renferme. Journal de l'Ecole Polytechnique, XVII^{e} Cahier, Tome X, p. 1, 1815. Complete works, second series, vo. I, p. 64, Paris, 1905.

[5] Galois' letter to A. Chevalier, see Works, published by Picard, Paris, 1897, p. 25.

[6] Encyclopédie des Sciences Mathématiques, tome I, vol. 1, p. 575.

A, B, C, ... of order a, b, c, ... respectively such that any element S can be obtained by a combination

$$S = A^{\alpha}B^{\beta}C^{\gamma}\ldots\ldots \qquad \text{where} \quad \begin{array}{l}\alpha=0,1,2,\ldots\ a-1,\\ \beta=0,1,2,\ldots\ b-1,\\ \gamma=0,1,2,\ldots\ c-1,\\ \text{etc.}\end{array}$$

where α designates the number of times the operator A has been combined with itself, β the number of times operator B has been combined with itself[7]) etc. Such a system of generators is called a base of an abelian group. It can be determined in several ways. For instance Kronecker chose them in such a way that if a, b, c, ... are taken in a certain order each of these numbers is a divisor of all the preceding ones, while Frobenius and Stickelberger have shown that they can all be put equal to primes, or powers of primes, all of which are divisors of the order of the group[8]) They then form what are known as the invariants of an abelian group. Jordan developed the idea of linear groups in which the congruence concept is made use of. This has been extended by Frobenius and Dickson within the last few years, but as the subject is approached from the viewpoint of the Galois imaginaries, which will be mentioned again somewhat later, it does not fall into close contact with the following developements.

Turning to the concept of a modulus we find the term defined by Gauss in the first two articles of his Disquisitiones Arithmeticae, published at Leipzig in 1801. He defines two numbers a and b congruent to modulus c when a-b is divisible by c. This idea he later extended to congruences of higher degrees, that is of the form $f_1(x)\equiv f_2(x)$, mod p, where $f_1(x)$ and $f_2(x)$ are rational, integral functions of x with rational coefficients. The object is to determine what values when substituted for x give us a numerical congruence of the form $a\equiv b$, mod p, where p is a rational, prime integer. The article is entitled "Disquisitiones Generales de Congruentiis"[9]), and was not published during Gauss' life. In it he obtains several theorems concerning the factorization of a function, mod p, the most important one being that

[7]) Encyclopédie des Sciences Mathématiques, tome I, vol. 1, pp. 601-602.
[8]) See Crelle's Journal, vol. 86 (1879), p. 219.
[9]) See Gauss' Werke vol. II, Göttingen, 1876, p. 212.

any $f(x)$ can be factored in but one way, mod p. Cauchy in an article entitled "Sur la Résolution des Equivalences"[10]) made an extensive study of the conditions that an integral, rational function of x with integral coefficients may have roots when taken modulo p, especially for functions of the second, third, and fourth degrees. Galois introduced the theory of the Galois imaginaries, by which every function, mod p, has as many roots as its degree even when it is irreducible in the rational realm. It is from this standpoint that functions of x are often studied with respect to a numerical modulus. The first case in which we have the idea of a double modulus introduced, although in a sense entirely different from the one in which we use it today is in an article by Th. Schoenemann[11]) in which the modulus (p,α) is used. The author's definition of this modulus, which he does not call double modulus, is that if α is a root of $f(x)$ and if $\psi(\alpha)=\varphi(\alpha)+p\theta(\alpha)$, then $\psi(\alpha)\equiv\varphi(\alpha)$, mod (p,α). Furthermore we have $f_1(x)\equiv f_2(x)$, mod (p,α), if all the coefficients of the two functions are functions of α, and the coefficients of equal powers are congruent, mod (p,α). Dedekind was the first one to define a double modulus in the sense now used.[12]) He defines two rational integral functions of x with integral coefficients, say $F_1(x)$ and $F_2(x)$, congruent modd $(\psi(x),p)$, where $\psi(x)$ is a rational integral function of x with integral coefficients, and p is a rational prime integer, whenever

$$F_1(x) = F_2(x) + \psi(x)\xi(x) + p\theta(x).$$

From this he proceeds to find the roots of a congruence of the form $N_0y^n + N_1y^{n-1}+ \ldots\ldots + N_n \equiv 0$, modd $(\psi(x),p)$, where the various N are rattional integral functions of x with integral coefficients, and $N_0 \not\equiv 0$.

Some work has already been done in applying the group idea to a residue system of integers with respect to a modulus m, where m is a rational integer, the group formed by the integers prime to m having been known for a long time. Some of its properties are given by Weber.[13]) Among the work done

[10]) Sur la Résolution des Equivalences dont les modules se réduisent à des nombres premiers, 1829, Paris.

[11]) Crelle's Journal, vol. 31, 1846, p. 269, vo. 32, 1846, p. 93.

[12]) Crelle's Journal, vol. 54, 1857, pp. 2,7.

[13]) Weber, Algebra. Vol. II, p. 66.

in the last few years is that of G.A. Miller, who has treated the questions of quadratic residues, the Euler function, and all the groups formed by the residues of the modular system, mod m.[14]) He has also found the invariants of the residue group formed with respect to modd (x^n, p) besides proving that the group of residues, modd $(\psi(x), p)$, that contains the operator 1 is made up of the product of residue groups containing 1 of the the moduli $(\varphi_1(x), p)$, $(\varphi_2(x), p)$, ... $(\varphi_n(x), p)$, where all the $\varphi(x)$ functions are irreducible, mod p, and $\psi(x)$ is equal to their product, mod p.[15]) Among other results he also obtained the theorem that all rational integers of a complete residue system, mod m, where m is a positive, rational integer, that have the same greatest common divisor d with m form an abelian group when m/d is prime to these integers, but not otherwise. It will be the object of this paper to extend this theorem to the residue system of a double modulus.

[14]) American Journal of Mathematics, 1905, vol. 31, p. 277.

[15]) Archiv fuer Mathematik und Physik, vol. 15, 1909, p. 115.

PROOF.

In dealing with a double modulus $(\psi(x),m)$ we have m a positive rational integer and $\psi(x)$ a rational, integral function of x with integral coefficients. In fact no other kind of function will be considered in this paper, and for the sake of brevity we will designate all functions as polynomials. Conversely when we speak of a polynomial we shall understand a function fulfilling the requirements laid down for $\psi(x)$. We shall define two polynomials as congruent to each other, modd $(\psi(x),m)$, that is

$$F_1(x) \equiv F_2(x) \qquad \text{modd } (\psi(x),m)$$

when $$F_1(x) = F_2(x) + \psi(x)\xi(x) + m\vartheta(x),$$

where all terms in the equation besides the m are polynomials. This includes as a special case the definition given above of Dedekind for the modd $(\psi(x),p)$, where $m=p$ a rational prime integer. From this equation it follows immediately that

$$F_1(x) \equiv F_2(x) + \psi(x)\xi(x) \qquad \text{mod } m.$$

All polynomials congruent to each other, modd $(\psi(x),m)$, form a residue class. That polynomial in a residue class whose degree is less than the degree of $\psi(x)$, and whose coefficients are positive, rational integers less than m, is the least residue of its class. Hereafter $f(x)$ will designate a least residue, while $F(x)$ will stand for any polynomial. To find the least residue of any polynomial $F(x)$, modd $(\psi(x),m)$, we divide $F(x)$ by $\psi(x)$, mod m, and take the coefficients of the remainder modulo m so that they are all positive and less than m. This gives the relation

$$F(x) = f(x) + \psi(x)\xi(x) + m\vartheta(x),$$

and consequently $$F(x) \equiv f(x) \qquad \text{modd } (\psi(x),m).$$

The single modulus m is but a special case of the double modulus $(\psi(x),m)$ for its residues $0,1,2, \ldots m-1$ are those residues of the double modulus where all powers of x above the zeroth have coefficients congruent to 0, mod m. We say that $f(x)$ is divisible by $f'(x)$ or contains the factor $f'(x)$, mod m, if there exists a polynomial $\zeta(x)$ such that $f(x) + m\zeta(x)$ is divisible by $f'(x)$, and the quotient be a polynomial. We know that Gauss has proven that any $F(x)$ can be broken up into factors in one way only, mod m, if m is a rational prime integer, but this is not true otherwise. Two polynomials are prime to each other, mod m, if their aggregate coefficients have no common divisor greater than 1, and the polynomials have no common factors with any prime divisor of m taken as modulus. A residue $f(x)$ is prime to modd $(\psi(x),m)$ if the coefficients of $f(x)$ and m have no common divisor greater than 1, and if $f(x)$ and $\psi(x)$ are prime to each other, mod m.

If we multiply any two $f(x)$ prime to modd $(\psi(x),m)$ the resulting $f(x)$ is also prime to this modulus, for let

$$f_1(x)f_2(x) \equiv f_3(x) \qquad \text{modd } (\psi(x),m),$$

where $f_1(x)$ and $f_2(x)$ are both prime to the modulus. If the coefficients of $f_1(x)$ have a common divisor, say d_1, take it out and write $f_1(x)$ as $d_1(\frac{f_1(x)}{d_1})$ and similarly if d_2 be highest common divisor of coefficients of $f_2(x)$ let us write this residue as $d_2(\frac{f_2(x)}{d_2})$. In neither $(\frac{f_1(x)}{d_1})$ nor $(\frac{f_2(x)}{d_2})$ have all the coefficients of either one polynomial a common divisor greater than 1, consequently in the product $f_1(x)f_2(x)$ which is equal to $d_1d_2(\frac{f_1(x)}{d_1})(\frac{f_2(x)}{d_2})$ by a theorem of Gauss[16]) the coefficients of $(\frac{f_1(x)}{d_1})(\frac{f_2(x)}{d_2})$ have no common divisor greater than 1, while d_1d_2 is not divisible by any factor of m because both d_1 and d_2 are prime to m. Consequently $f_1(x)f_2(x)$ is not divisible by m. The polynomials $f_3(x)$ and $\psi(x)$ must be prime to each other, mod m, for if p_i be any prime divisor of m we know that $f_1(x)$ and $f_2(x)$ can each be broken up into but one set of irreducible factors, mod p_i, all of which are contained in $f_1(x)f_2(x)$, mod p_i. Since $f_1(x)$ and $f_2(x)$ are prime to $\psi(x)$, mod m, neither of them has any factor $f'(x)$ in common with $\psi(x)$, mod p_i. Now if it were possible to factor $f_1(x)f_2(x)$, mod p_i, so as to include a divisor $f'(x)$ of $\psi(x)$ we would have two factorizations of $f_1(x)f_2(x)$, mod p_i, which we know is impossible. Moreover we can write our congruence in the form

$$f_1(x)f_2(x) \equiv f_3(x) + \psi(x)\xi(x) \qquad \text{mod } p_i,$$

for when an expression is divisible by m it is also divisible by every di-

[16]) The theorem referred to is: If $f_1(x)=a_0x^m+a_1x^{m-1}+\dots+a_m$, and $f_2(x)=b_0x^n+b_1x^{n-1}+\dots+b_n$, be any two integral functions of x, whose coefficients are rational integers, having in each case no common divisor, then the coefficients of the product of these functions $f(x)=f_1(x)\cdot f_2(x)=c_0x^{m+n}+c_1x^{m+n-1}+\dots+c_{m+n}$ are rational integers without a common divisor.

soe p_i of m. Now the left hand member of this congruence is not divisible by any factor $f'(x)$ of $\psi(x)$, mod p_i, while $\psi(x)$ in the right hand member is. Consequently $f_3(x)$ cannot contain any factor $f'(x)$ of $\psi(x)$, mod p_i, as the above congruence would then be impossible. Since this holds true for every prime divisor of m it must hold true for m used as modulus. Hence $f_3(x)$ is prime to modd $(\psi(x),m)$ and the product of any two residues prime to modd $(\psi(x),m)$ gives another residue prime to this modulus.

When we multiply any one residue prime to modd $(\psi(x),m)$ by all residues prime to this modulus we get back all of them. For if this were not true at least one product would have to be repeated. But that is impossible, for if

$$f_1(x)f_2(x) \equiv f_1(x)f_3(x) \equiv f_4(x) \qquad \text{modd } (\psi(x),m),$$

Then

$$f_1(x)[f_2(x)-f_3(x)] \equiv 0 \qquad \text{modd } (\psi(x),m).$$

Consequently all the coefficients of the left hand member must be divisible by m, or this member must be divisible by $\psi(x)$, mod m. Taking the first case we have by definition that $f_1(x)$ is not divisible by any divisor of m, consequently if this condition is to be fulfilled $f_2(x)-f_3(x)$ must be divisible by m. But since $f_2(x)$ and $f_3(x)$ are least residues their coefficients are all positive and less than m in value. Consequently the coefficients of the expression $f_2(x)-f_3(x)$ are all less than m in value, and consequently conditions are satisfied only when $f_2(x)=f_3(x)$. If $f_1(x)[f_2(x)-f_3(x)]$ is divisible by by $\psi(x)$, mod m, then for any prime divisor p_i of m in the congruence

$$f_1(x)[f_2(x)-f_3(x)] \equiv \psi(x)\xi(x) \qquad \text{mod } p_i$$

some factor of $\psi(x)$ must be contained in $f_1(x)$, since $f_2(x)-f_3(x)$ is of lower degree than $\psi(x)$. Since $f_1(x)$ is prime to $\psi(x)$, mod m, this is impossible. Hence $f_1(x)[f_2(x)-f_3(x)]$ is not divisible by $\psi(x)$, mod m, and multiplying one residue prime to modd $(\psi(x),m)$ by all those prime to this modulus gives back all in the set. Since the commutative and associative laws of multiplication hold for algebraic polynomials we see that the residues prime to modd $(\psi(x),m)$ form an abelian group. As 1 is prime to the modulus it is evidently in this group and acts as its unit operator. As an example of such an abelian group we may mention the group

$$4x+3, \quad 3x+3, \quad 5, \quad 1. \qquad \text{modd } (x^2+3x+2=(x+1)(x+2),6).$$

Let us now consider the special case when the modulus is of the form

$(\varphi(x),p)$, where p is a positive rational prime and $\varphi(x)$ is a polynomial irreducible, mod p, of degree ν. Evidently the coefficient of the νth power of $\varphi(x)$ is 1, for otherwise this polynomial may be regarded as the product of this coefficient and some other irreducible polynomial, mod p, whose coefficient for the νth power is 1. The total number of residues in the system is p^ν, for $f(x)$ is of the form $a_0x^{\nu-1} + a_1x^{\nu-2} + \ldots\ldots + a_{\nu-1}$, and since there are ν coefficients each of which can assume p values, mod p, we see that there are p^ν combinations. Since p is a prime and $\varphi(x)$ is irreducible, mod p, it is evident that the whole residue system represented by the least residues must be prime to the modulus, excepting the zero. Consequently we have an abelian group of order $p^\nu-1$. It will now be shown that this group is a cyclic group. Suppose that $f_1(x)$, one of the residues prime to modd $(\varphi(x), p)$, is of order μ where μ is a divisor of $p^\nu-1$. Then $f_1(x)$, $[f_1(x)]^2$, ..., $[f_1(x)]^\mu=1$ will all be distinct residues. Let ε represent any one of the numbers 1, 2, ... μ. Hence

$$[f_1(x)]^\mu \equiv 1 \qquad \text{modd } (\varphi(x),p)$$
$$[f_1(x)]^{\varepsilon\mu} \equiv 1 \qquad \text{"}$$
$$[(f_1(x))^\varepsilon]^\mu \equiv 1 \qquad \text{"}$$
$$\text{(I)} \qquad [(f_1(x))^\varepsilon]^\mu - 1 \equiv 0. \qquad \text{"}$$

From the theory of congruences we know that any function in x can be factored in only one way, mod p. An extension of this theorem with a purely algebraic proof is given by Serret[17] in the following theorem and corollary: If X_1, X_2, ... X_n represent least residues of modd $(\varphi(x),p)$, and if we have $F(X)=A_0X^n+A_1X^{n-1}+\ldots+A_n$ be an integral rational function whose coefficients are functions of the residues of the residue system of modd $(\varphi(x),p)$, then if after substituting X_1, X_2, ... X_n for X in $F(X)$ the results are all divisible by $\varphi(x)$, mod p, we get identically

$$F(X) = A_0(X-X_1)(X-X_2)\ldots\ldots(X-X_n) + \varphi(x)\xi(X,x) + p\theta(X,x),$$

where $\xi(X,x)$ and $\theta(X,x)$ are integral rational functions with rational integral coefficients of the two variables X and x. The corollary states: If $F(X)$ gives 0 for more than n values of X it is identically equal to zero.

[17]) Serret, Cours d'Algèbre Superieure, sixth edition, vol. II, pp. 129-132.

What the theorem states is that if we take $F(X)$ with respect to the double modulus $(\varphi(x),p)$ it cannot have more roots than its degree, and hence can be factored in but one way. From this it follows that equation (I) which may be written as

$$X^{\mu} - 1 \equiv 0 \qquad \text{modd } (\varphi(x),p)$$

cannot have more than μ solutions. Since $f_1(x)$, $[f_1(x)]^2$, ... $[f_1(x)]^{\mu}$ when raised to the μ power all satisfy the congruence there can be no other residues that satisfy it. Now let the order of $[f_1(x)]^{\varepsilon}$, where $\varepsilon=1,2,\ldots \mu$, be τ. Now $\tau\varepsilon$ is a multiple of μ since $f_1(x)$ is of order μ. If ε is prime to μ we get $\tau=\mu$, otherwise if μ and ε have the highest common divisor d

$$[[f_1(x)]^{\varepsilon}]^{\frac{\mu}{d}} \equiv [[f_1(x)]^{\frac{\varepsilon}{d}}]^{\mu} \equiv 1 \qquad \text{modd } (\varphi(x),p),$$

and consequently $f_1(x)$ is of order lower than μ. Since there are only $\varphi(\mu)$ numbers in the set $1,2,\ldots\mu$, that are prime to μ, there are but $\varphi(\mu)$ residues in the system, modd $(\varphi(x),p)$, that are of order μ. From this it follows direcly that there is but one subgroup of every order μ in the abelian group of order $p^{\nu}-1$, modd $(\varphi(x),p)$. For if this group contained two subgroups of the same order μ, we would have more than $\varphi(\mu)$ operators of order μ, this number being contained in one of the subgroups, and hence the second subgroup would have to be generated by an operator found in the first one, in which case the two are identical. But when an abelian group has but one subgroup of every order it is a cyclic group, in this case of order $p^{\nu}-1$. An example of such a group is seen in the following group generated by $x+1$, modd $(x^2+2,5)$. The order of the group is $p^{\nu}-1=5^2-1=24$.

1) $x+1$	7) $3x+3$	13) $4x+4$	19) $2x+2$
2) $2x+4$	8) $x+2$	14) $3x+1$	20) $4x+3$
3) x	9) $3x$	15) $4x$	21) $2x$
4) $x+3$	10) $3x+4$	16) $4x+2$	22) $2x+1$
5) $4x+1$	11) $3x+3$	17) $x+4$	23) $3x+2$
6) 3	12) 4	18) 2	24) 1.

It is noticed that the integers $1,2,\ldots p-1$ form a subgroup of the group, and this is true in general for any group taken modd $(\varphi(x),p)$. A complete list of groups of modd $(\varphi(x),p)$ of order less than 12 is given by G. A.Miller[18]). Summing up the results obtained we have the

THEOREM: ALL THE LEAST RESIDUES OF A COMPLETE RESIDUE SYSTEM, MODD $(\psi(x),m)$, THAT ARE PRIME TO THIS MODULUS FORM AN ABELIAN GROUP. WHEN THE MODULUS IS OF THE FORM $(\varphi(x),p)$ WHERE p IS A POSITIVE RATIONAL PRIME INTEGER AND $\varphi(x)$ IS AN IRREDUCIBLE POLYNOMIAL OF DEGREE ν WITH RESPECT TO MODULUS p, ALL THE LEAST RESIDUES EXCEPTING THE 0 FORM A CYCLIC GROUP OF ORDER $p^\nu-1$.

Let us now consider those least residues that are not prime to modd $(\psi(x),m)$. For the present let us confine ourselves to the case where $m=p^\alpha$, where p is a positive rational prime. Whenever two polynomials are congruent, modd $(\psi(x),p^\alpha)$, let us say

$$F_1(x) \equiv F_2(x) \qquad \text{modd } (\psi(x),p^\alpha)$$

and

$$\psi(x) \equiv \psi'(x)\psi''(x) \qquad \text{mod } p^\alpha,$$

Then since

$$F_1(x) = F_2(x) + \psi(x)\Xi(x) + p^\alpha\theta(x)$$

can be written

$$F_1(x) = F_2(x) + \psi'(x)\psi''(x)\Xi(x) + p^\alpha\theta'(x)$$

we have

$$F_1(x) \equiv F_2(x) \qquad \text{modd } (\psi'(x),p^\alpha).$$

Now take a modulus $(\psi(x),p^\alpha)$ where $\psi(x)$ contains the factor $\psi''(x)$, mod p^0, and where the resulting quotient $\psi'(x)$ is prime to $\psi''(x)$, mod p^α. Take all the least residues, modd $(\psi(x),p^\alpha)$, that contain the factor $\psi''(x)$, mod p^α, but are prime to modd $(\psi'(x),p^\alpha)$. Although $\psi(x)$ can as a rule be factored in more than one way, mod p^α, all the different factorizations always reduce to the same one, mod p, and as we by definition determine whether a residue is prime to modd $(\psi'(x),p^\alpha)$ by seeing whether it is prime to modd $(\psi'(x),p)$, the fact that a polynomial may be reducible in more than one way, mod p^α, does not enter. If we multiply, modd $(\psi(x),p^\alpha)$, two $f(x)$ of the set of residues that contain the factor $\psi''(x)$, mod p^α, and that are prime to modd $(\psi'(x),p^\alpha)$, we get another $f(x)$ of this set, for if $f_1(x)$ and $f_2(x)$ are any two residues of the set that fulfill the conditions and

$$f_1(x)f_2(x) \equiv f_3(x) \qquad \text{modd } (\psi(x),p^\alpha)$$

we have also just shown that

$$f_1(x)f_2(x) \equiv f_3(x) \qquad \text{modd } (\psi'(x),p^\alpha),$$

[18]) Archiv fuer Mathematik und Physik, vol. 15, 1909, p. 115.

where $f_1(x)$ and $f_2(x)$ are both prime to modd $(\psi'(x), p^\alpha)$ by assumption, consequently $f_3(x)$ is also prime to it. Moreover the congruence preceding the last one may be written

$$f_1(x)f_2(x) \equiv f_3(x) + \psi(x)\xi(x) \qquad \text{mod } p^\alpha,$$

or transposing

$$f_1(x)f_2(x) - \psi(x)\xi(x) \equiv f_3(x) \qquad \text{mod } p^\alpha,$$

the left hand member of which is divisible by $\psi''(x)$, mod p^α, consequently the right hand member must also be divisible by $\psi''(x)$, mod p^α. Consequently the product of any two residues of the set gives another residue of the set.

Moreover the product of any one of this set, modd $(\psi(x), p^\alpha)$, by all of the set gives back all of the set, for were this not true at least one of the residues in the set would be repeated in the products, let us say that

$$f_1(x)f_2(x) \equiv f_1(x)f_3(x) \equiv f_4(x) \qquad \text{modd } (\psi(x), p^\alpha)$$

each of the residues being a residue of our set. From this

$$f_1(x)f_2(x) \equiv f_1(x)f_3(x) \qquad \text{modd } (\psi'(x), p^\alpha)$$

from which it follows since $f_1(x)$, $f_2(x)$, and $f_3(x)$ are residues of the group of residues prime to modd $(\psi'(x), p^\alpha)$ that

$$f_2(x) \equiv f_3(x) \qquad \text{modd } (\psi'(x), p^\alpha).$$

But no two of our set reduce to the same residue, modd $(\psi'(x), p^\alpha)$, for if any two of them, say $f_2(x)$ and $f_3(x)$ were congruent, modd $(\psi'(x), p^\alpha)$ we would have

$$\frac{f_2(x) + p^\alpha\theta_1(x)}{\psi''(x)} = \frac{f_3(x) + p^\alpha\theta_2(x)}{\psi''(x)} + \psi'(x)\xi(x) + p^\alpha\theta(x),$$

or $$f_2(x) + p^\alpha\theta_1(x) = f_3(x) + p^\alpha\theta_2(x) + \psi(x)\xi(x) + p^\alpha\theta'(x),$$

$$f_2(x) = f_3(x) + \psi(x)\xi(x) + p^\alpha\theta''(x),$$

hence $$f_2(x) \equiv f_3(x) \qquad \text{modd } (\psi(x), p^\alpha),$$

which is contrary to our assumptions. Consequently when we multiply one residue of the set by all of the set, we get back all of the set. Since the commutative and associative laws hold for the multiplication of algebraic polynomials we have proven that our set forms an abelian group, modd $(\psi(x), p^\alpha)$. We know that to every residue of our set, modd $(\psi(x), p^\alpha)$, there corresponds a residue prime to modd $(\psi'(x), p^\alpha)$. Conversely to every residue prime to modd $(\psi'(x), p^\alpha)$ there corresponds a residue of our set, modd $(\psi(x), p^\alpha)$, which is obtained by multiplying the residue prime to modd $(\psi'(x),p^\alpha)$ by $\psi''(x)$, mod p^α, the residue thus obtained being of degree less than the degree of $\psi(x)$ and in every way satisfying the requirements of our set, modd $(\psi(x),p^\alpha)$. Hence there is a one to one correspondence between the two sets of residues, and the groups formed are simply isomorphic. When we put $\psi''(x)$ equal to 1 we get the group of residues prime to modd $(\psi(x),p^\alpha)$, for in this case $\psi(x)=\psi'(x)$.

It will now be shown that the residues obeying the rules laid down above are the only ones that form groups. All the residues of the complete residue system, modd $(\psi(x),p^\alpha)$, can be placed into one of the following classes, when $\psi''(x)$ will designate the greatest common divisor of the residue and $\psi(x)$, mod p^α:

1) Residues divisible by $\psi''(x)$, mod p^α, and prime to modd $(\psi'(x),p^\alpha)$, where $\psi(x)\equiv\psi'(x)\psi''(x)$, mod p^α. This includes the residues prime to modd $(\psi(x),p^\alpha)$, for the special case that $\psi''(x)=1$.
2) Residues divisible by p.
3) Residues divisible by $\psi''(x)$, mod p^α, but not prime to modd $(\psi'(x),p^\alpha)$ because they have factors in common, mod p^α.
4) Residues divisible by $\psi''(x)$, mod p^α, but not prime to modd $(\psi'(x),p^\alpha)$ because they have factors in common with $\psi'(x)$, mod p, but not mod p^α.

All residues of class 1) have been shown to belong to groups. If a residue of class 2) be taken and raised to a sufficiently high power it becomes divisible by p^α, and hence becomes congruent to 0, modd $(\psi(x),p^\alpha)$. Since 0 cannot occur in a group of residues, modd $(\psi(x),p^\alpha)$, we see that the residues of class 2) do not belong to any group. Now let us consider class 3). If there is any residue $f(x)$ in this class that is contained in a group, modd $(\psi(x),p^\alpha)$, it must repeat itself after being raised to a sufficiently high power because the number of residues is finite. Let us suppose that

$$[f(x)]^\kappa \equiv f(x) \qquad \text{modd } (\psi(x),p^\alpha),$$

and for the sake of convenience let us write

$$\text{(I)} \qquad f(x)[f(x)]^{\kappa-1} \equiv f(x) \qquad \text{modd } (\psi(x),p^\alpha).$$

Since $f(x)$ and $\psi(x)$ both contain the factor $\psi''(x)$, mod p^α, and $\psi(x)$ is congruent to $\psi'(x)\psi''(x)$, mod p^α, there exist polynomials $\theta_i(x)$ such that

$$f(x) + p^\alpha\theta_1(x) = \psi''(x)[f'(x) + p^\alpha\theta_1'(x)]$$

and
$$\psi(x) + p^\alpha\theta_2(x) = \psi''(x)[\psi'(x) + p^\alpha\theta_2'(x)],$$

where $f'(x)$ is the least residue obtained after dividing $f(x)$ by $\psi''(x)$, modd $(\psi(x),p^\alpha)$. Now (I) can be written

$$f(x)[f(x)]^{\kappa-1} = f(x) + \psi(x)\xi(x) + p^\alpha\theta(x)$$

and substituting, leaving away the (x) of the various functions for sake of convenience, and denoting it merely by the letter f, ψ, etc. we have

$$[\psi''(f'+p^\alpha\theta_1')-p^\alpha\theta_1]f^{\kappa-1} = \psi''(f'+p^\alpha\theta_1')-p^\alpha\theta_1+\xi[\psi''(\psi'+p^\alpha\theta_2')-p^\alpha\theta_2]+p^\alpha\theta,$$

which upon collecting the terms in $\psi''(x)$ on the left hand member is

(I') $\quad \psi''[f'(f^{\kappa-1}+p^\alpha f^{\kappa-1}\theta_1'-f'-p^\alpha\theta_1'-\xi\psi'-p^\alpha\xi\theta_2'] = p^\alpha[\theta_1 f^{\kappa-1}-\theta_1-\xi\theta_2+\theta].$

Both members of the equation are divisible by $\psi''(x)$, and since $\psi''(x)$ is not divisible by p, for the residues of this class although divisible by $\psi''(x)$, mod p^α, are not divisible by p, we have

$$f'f^{\kappa-1} + p^\alpha f^{\kappa-1}\theta_1' - f' - p^\alpha\theta_1' - \xi\psi' - p^\alpha\xi\theta_2' = p^\alpha\theta'',$$

where $p^\alpha\theta''(x)$ is the quotient obtained in the right hand member of (I') after dividing by $\psi''(x)$. Collecting the terms in p^α and writing out in full we have
$$f'(x)[f(x)]^{\kappa-1} - f'(x) - \xi(x)\psi'(x) = p^\alpha\theta'''(x)$$
or
$$f'(x)[f(x)]^{\kappa-1} \equiv f'(x) \qquad \text{modd } (\psi'(x),p^\alpha).$$

The residue $f'(x)$ has no divisors in common with $\psi'(x)$, mod p^α, since we divided out their greatest common divisor, mod p^α. On the other hand $f(x)$ does have factors in common with $\psi'(x)$, mod p^α, because $f(x)$ is in class 3). Transposing in the last congruence we get

(II) $\quad f'(x)[(f(x))^{\kappa-1} - 1] \equiv 0 \qquad \text{modd } (\psi'(x),p^\alpha).$

In order that this congruence may be true the coefficients of the quantity within the brackets must be divisible by p^α, or by the quantity $\psi'(x)$, mod p^α, since neither condition holds for $f'(x)$, modd $(\psi'(x),p^\alpha)$. If the coefficients are all divisible by p^α we have

(II') $\quad [f(x)]^{\kappa-1} - 1 = p^\alpha\theta(x).$

There is a theoremdealing with the division of polynomials that states[19]: If F and φ are two polynomials in x of which φ is not identically zero,there

[19]) Bocher, Introduction to Higher Algebra, p. 161

exists one, and only one, pair of polynomials, Q and R, which satisfy the identity
$$F(x) \equiv Q(x)\varphi(x) + R(x),$$
and such that either $R\equiv 0$, or the degree of R is less than the degree of φ. The coefficients of these polynomials may be imaginaries, fractions, or integers. Putting in $p^{\alpha}\theta(x)$ for the F polynomial and $p^{\alpha}\psi'(x)$ for the φ polynomial we have
$$\text{(III)} \qquad p^{\alpha}\theta(x) = p^{\alpha}Q(x)\psi'(x) + R(x).$$
The term $R(x)$ must be divisible by p^{α} because the other two are. The coefficients of $\theta(x)$ are all integers by the assumption made that the coefficients of the quantity within the brackets of (II) are all divisible by p^{α}. Those of $\psi'(x)$ are also all integers. Since $R(x)$ is of degree less than $\psi'(x)$ the polynomial $Q(x)$ must have nothing but rational integers for coefficients, otherwise there would be some term in the right hand member of (III) with a coefficient that is not a rational integer, while the term of corresponding degree in the left hand member has a coefficient that is a rational integer, which cannot be. Finally if $\theta(x)$, $Q(x)$, and $\psi'(x)$ all have rational integers as coefficients the same must be true of $R(x)$. Substituting in (III) the left hand member of (II') we get, putting $R(x)=p^{\alpha}R'(x)$, and $p^{\alpha}Q(x)=Q'(x)$,
$$[f(x)]^{\kappa-1} - 1 = Q'(x)\psi'(x) + p^{\alpha}R'(x),$$
or in other words
$$[f(x)]^{\kappa-1} \equiv 1 \qquad \text{modd } (\psi'(x),p^{\alpha}),$$
which is impossible since $f(x)$ and $\psi'(x)$ have a common factor, mod p^{α}. Hence not all the coefficients of $[(f(x))^{\kappa-1} - 1]$ are divisible by p^{α}. Nor is the polynomial divisible by $\psi'(x)$, mod p^{α}, for then we have
$$[f(x)]^{\kappa-1} - 1 = \xi(x)\psi'(x) + p^{\alpha}\theta(x)$$
or
$$[f(x)]^{\kappa-1} \equiv 1 \qquad \text{modd } (\psi'(x),p^{\alpha}).$$
This is impossible, hence the congruence (II) is not true, i.e. $f(x)$ when raised to powers does not repeat itself, modd $(\psi(x),p^{\alpha})$, hence, since $f(x)$ was any residue of class 3, the residues of class 3) are not contained in groups, modd $(\psi(x),p^{\alpha})$.

In class 4) if any residue $f(x)$ is a member of a group, modd $(\psi(x),p^{\alpha})$, it must repeat itself after being raised to a sufficiently high power with respect to this modulus, i.e. $[f(x)]^\kappa \equiv f(x)$, modd $(\psi(x), p^\alpha)$, must be true for some value of κ. Transposing

$$\text{(IV)} \quad f(x)[(f(x))^{\kappa-1} - 1] \equiv 0 \qquad \text{modd } (\psi(x), p^\alpha).$$

Here $f(x)$ and $\psi(x)$ have no factors in common, mod p^α, although they have, mod p. As in the case of class 3) we must now prove that if $f(x)$ is in a group the quantity within the brackets is congruent to 0, modd $(\psi(x), p^\alpha)$, i.e. either all its coefficients are divisible by p^α, or it is divisible by $\psi(x)$, mod p^α, since the $f(x)$ outside the brackets is not divisible by p, nor has it any factors in common with $\psi(x)$, mod p^α. To proof is the same as for class 3) to show that congruence (IV) cannot be true, and that for this reason no residue of class 4) is contained in a group of residues, modd $(\psi(x), p^\alpha)$. From these considerations we have the following

THEOREM: A NECESSARY AND SUFFICIENT CONDITION THAT A SET OF RESIDUES OF THE COMPLETE RESIDUE SYSTEM, MODD $(\psi(x), p^\alpha)$, FORM AN ABELIAN GROUP IS THAT THE SET BE COMPOSED OF ALL THOSE RESIDUES THAT HAVE THE SAME HIGHEST COMMON DIVISOR $\psi''(x)$ WITH $\psi(x)$, MOD p^α, AND ARE PRIME TO MODD $(\psi'(x), p^\alpha)$, WHERE $\psi'(x)\psi''(x) = \psi(x)$, MOD p^α. SUCH A GROUP OF RESIDUES IS SIMPLY ISOMORPHIC TO THE GROUP OF RESIDUES, MODD $(\psi'(x), p^\alpha)$, THAT IS COMPOSED OF RESIDUES PRIME TO THIS MODULUS.

The following examples will illustrate the theorem:

Ex. 1. Modd $(x^3+2x^2+3x+2 = (x+1)(x+2)(x+3), 4 = 2^2)$. The residues $x+2$, $3x+2$, x^2, $3x^2$, $2x^2+x+2$, $2x^2+3x+2$, x^2+2x, and $3x^2+2x$ form an abelian group, all of them containing with x^3+2x^2+3x+2 the highest common divisor $x+2$, mod 4, and all being prime to modd $(x^2+3 = (x+1)(x+3), 4)$. With respect to this modulus they become 1, 3, x, 3x, x+2, 2x+1, 2x+3, 3x+2, which is the group of residues prime to this modulus. Consequently the two groups are simply isomorphic.

Modd $(x^3+2x^2+3x+2 = (x+1)(x+2)(x+3), 4 = 2^2)$. The residues x^2+3 and $3x^2+1$ form a group, both having with x^3+2x^2+3x+2 the greatest common divisor x^2+3, mod 4, and are prime to modd $(x+2, 4)$. They are simply isomorphic to the group of residues prime to this latter modulus, namely 1, 3, and reduce to this group with respect to this modulus.

Ex. 2. Modd $(x^3+4x^2+2x+8 = (x+1)(x+5)(x+7), 9 = 3^2)$. The residues x^2+8x+7, $2x^2+7x+5$, $4x^2+5x+1$, $5x^2+4x+8$, $7x^2+2x+4$, and $8x^2+x+2$ form a group. All of them have with x^3+4x^2+2x+8 the greatest common divisor $(x+1)(x+7) = x^2+8x+7$, mod 9. The group is simply isomorphic to the group 1, 2, 4, 5, 7, 8, prime to modd $(x+5,9)$, and since all its residues are prime to this modulus they reduce to this second group when taken with respect to the latter modulus.

Now let us consider the case of modd $(\psi(x),m)$, where $m=p_1^{\alpha_1}\dots p_i^{\alpha_i}\dots p_r^{\alpha_r}$, the different p's all being rational prime integers, and $\alpha_1, \dots \alpha_r$ all being positive rational integers. It will be shown that the necessary and sufficient condition that a set of residues, modd $(\psi(x),m)$, form a group is that they form groups with respect to the moduli $(\psi(x),p_1^{\alpha_1})$, ... $(\psi(x),p_r^{\alpha_r})$. A congruence holding for modd $(\psi(x),m)$ is evidently true for modd $(\psi(x),p_i^{\alpha_i})$, for when we write the congruence as an equation we can write for $m\cdot\theta(x)$ the term $p_i^{\alpha_i}(m'\theta(x))$, where $m=m'p_i^{\alpha_i}$. From this it follows that if a residue of modd $(\psi(x),m)$ is in a group it cannot have all its coefficients divisible by a lower power of any factor p_i of m than p_i is contained in m, for otherwise when we raise the residue to powers, modd $(\psi(x),p_i^{\alpha_i})$, a residue divisible by $p_i^{\alpha_i}$, hence congruent to 0 with respect to this modulus. From this it follows that it cannot repeat itself, modd $(\psi(x),p_i^{\alpha_i})$, and hence not modulo $(\psi(x),m)$. Consequently such a residue cannot be in a group of residues, modd $(\psi(x),m)$. If we take a set of residues, modd $(\psi(x),m)$, that form groups with respect to the moduli $(\psi(x),p_1^{\alpha_1})$, $(\psi(x),p_2^{\alpha_2})$, ... $(\psi(x),p_r^{\alpha_r})$, it is evident that they may all have all of their coefficients divisible by a power of some factor p_i of m if this power be of a degree at least as great as p_i is contained in m, for then all the residues of our set become congruent to 0, modd $(\psi(x),p_i^{\alpha_i})$, and as 0 forms a group of order 1 with respect to any modulus we have no contradiction. The product of any two residues of our set will give a third one of our set, for if it were not of the set there would be some modulus $(\psi(x),p_i^{\alpha_i})$ where it would not be an operator in the same group as the first two, which is impossible as proven by the last theorem. Furthermore if any one residue of the set, modd $(\psi(x),m)$, be multiplied by all the residues of such a set we get back the whole set, modd $(\psi(x),m)$. If this were not true at least one product would have to be repeated, and let us suppose that $f_1(x)$, $f_2(x)$, $f_3(x)$, and $f_4(x)$ are of the set and that

$$(V) \qquad f_1(x)f_2(x) \equiv f_1(x)f_3(x) \equiv f_4(x) \qquad \text{modd } (\psi(x),m).$$

This congruence must hold for every modd $(\psi(x),p_i^{\alpha_i})$, and hence

$$f_1(x)f_2(x) \equiv f_1(x)f_3(x) \qquad \text{modd } (\psi(x),p_i^{\alpha_i}),$$

THE UNIVERSITY OF ILLINOIS

The thesis by Mr. Kircher appears to me to be a very creditable piece of work, which is entirely satisfactory as an A. M. thesis. The number of new results is considerable and the developments relating to known work are of a high order

G. A. Miller

May 25, 1912.

from which it follows, since these residues form a group with respect to this modulus, that

$$f_2(x) = f_3(x) + \xi(x)\psi(x) + p_i^{\alpha_i}\theta_i(x).$$

But $\psi(x)$ is of higher degree than any of the $f(x)$ polynomials, consequently $\xi(x)=0$ and

$$f_2(x) = f_3(x) + p_i^{\alpha_i}\theta_i(x).$$

This holds for every value of i from 1 to r, and since $p_1, p_2, \ldots p_r$ are all prime to each other $f_2(x)$ and $f_3(x)$ must differ by some function $\theta'(x)$ containing all the factors $p_1^{\alpha_1}, \ldots. p_r^{\alpha_r}$, or in other words

$$f_2(x) = f_3(x) + m\theta(x).$$

Consequently $f_2(x) \equiv f_3(x) \qquad \text{modd } (\psi(x),m),$

which is contrary to our assumptions. Consequently one of the set multiplied by all of them gives back all of them, modd $(\psi(x),m)$. Since the commutative and associative laws of multiplication hold for algebraic polynomials we see that the set forms an abelian group. That the conditions stated are also necessary we see from the fact that if for some modd $(\psi(x),p_i^{\alpha_i})$ our set does not form a group we do not get back the whole set, modd $(\psi(x),p_i^{\alpha_i})$, when we multiply all of the set into a certain one of the set, and hence we do not get back the whole set, modd $(\psi(x),m)$. Consequently the conditions given are also necessary. From the preceeding argument we get the

THEOREM: A NECESSARY AND SUFFICIENT CONDITION THAT A SET OF RESIDUES TAKEN MODD $(\psi(x),m)$ FORM A GROUP, WHERE $m=p_1^{\alpha_1}p_2^{\alpha_2}\ldots p_i^{\alpha_i}\ldots p_r^{\alpha_r}$, IS THAT THEY FORM A GROUP WITH RESPECT TO EACH OF THE MODULI $(\psi(x),p_1^{\alpha_1})$, ... $(\psi(x),p_i^{\alpha_i})$, ... $(\psi(x),p_r^{\alpha_r})$.

From this theorem and the preceeding discussion and proof we see that this is a generalization of the theorem given by G.A.Miller as stated at the beginning of this article. As a simple example illustrating the theorem we have

Ex. Modd $(x^2+3x+2=(x+1)(x+2),6)$. Take the residues $3x+2$ and $3x+4$. Here $6=2\times3$. Taking the $\psi(x)=x^2+3x+2$ with regard to the moduli 2 and 3 respectively we get the moduli $(x^2+x,2)$ and $(x^2+2,3)$. With respect to the first modulus our two residues reduce to x in each case, and as x forms a group of order1, modd $(x^2+x,2)$ this condition is satisfied. With respect to second modulus they reduce to group 1,2, which satisfies conditions modd $(x^2+2,3)$. Hence $3x+2$ and $3x+4$ form a group of order 2,modd$(x^2+3x+2,6)$,as is apparent.

BIBLIOGRAPHY.

Besides the references given in the foot note the following books and works were consulted:

1) The French Encyclopedia of Mathematics.

2) The German Encyclopedia of Mathematics.

3) Pascal's Repertorium der Mathematik.

4) Reid, L.W., The Elements of the Theory of Algebraic Numbers.

5) Burnside, The Theory of Groups.